



FEATURE ARTICLE

Thinking Outside the Box: Considering Wireless Networking and Remote Access

Wireless and remote communication today is a way of life. From laptops and netbooks to iPods and smart phones, today nearly every device is remote-ready. The demand for mobility and plethora of technologies are creating both challenges and opportunities for banking and IT professionals to provide safe and secure means of using this technology.

Planning for Mobility

Because so many wireless services and technologies are easily available, planning for their utilization is a business-critical process. Adoption of these devices has become easier to deploy and opened up access for employees to perform more and more of their work remotely and keep the corporate cross hairs on productivity. Banks have even been able to conduct detailed regulatory reviews without a single on-site visit. But these devices - and the data they connect to- can be vulnerable. Several recent events are stark evidence that these deployments can have recourse to security breaches and potential network hazards.

Before implementing any wireless or remote access, you should consult your IT and internal auditing professionals, and review any related security information from your respective regulatory agency (www.fdic.gov, www.ffiec.gov, www.occ.treas.gov). Each plan to utilize wireless or remote access also requires a detailed risk analysis to document the risks and means to mitigate them, and must be kept on file as for future regulatory audits and internal IT audits. Remember, if you adequately define, document and mitigate the risk, your IT audit and regulators will be happier.

There are many references, white papers, studies and examples available on the Internet regarding the considerations and risks for mobile banking, wireless remote user/customer access, but be sure to validate information with a reputable source. A good source of help is your core technology provider. The best providers have a wealth of highly trained, experienced professionals to consult.

Vigilance is Key

Wireless applications are so new that potential trouble spots are identified every day. Even if you aren't ignoring wireless security issues, you may not be paying enough attention to them.

Review each application's security needs in light of what the device does or doesn't provide. If there is a chance of risk, management must clearly understand and mitigate whether this type of access is allowed. If you're looking at thin-clients, for example, the built-in security may be getting better with each new version, but remember that it is still limited. A customized approach that allows you and your core and IT provider(s) to control the protection and encryption options is still your best option.

Building Long-term Success

If you want to offer wireless access for particular staff or customer needs (e.g., specific applications, a community room, customer kiosk, etc), consider if the source can be isolated from your internal network and corporate data. You may be able to use an inexpensive DSL, Cable or Wireless service exclusively for this purpose.

If you want a wireless or remote access to your network and data, ensure that you are consulting with the right people to choose the best commercial wireless technology available, and that it is set up according to reputable security best practices, including the latest encryption. Do not use easily identifiable or revealing information for base stations or access points. Consult with your core technology provider to assist with the product selection, installation and support. Ensure that solutions you consider are reputable, viable, will accept some responsibility or liability for loss and provide a level of assurance that their solution is indeed complaint and state of the art.

Thinking (and working) outside the box can give your bank more freedom and productivity, day to day. But remember to also think outside the box when considering the security of implementing wireless and remote technologies. Find out about the risks as well as the benefits, and how your current network and core technology providers can help.

Robert R. Ross is CSO and Vice President of Network/Technical Services at Hutchinson, Kansas-based DCI (www.datacenterinc.com), a nationwide provider advanced core processing and technology solutions to the banking industry. For more information, visit www.datacenterinc.com or call 620.694.6800.